AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original ☐

CLERK'S OFFICE
A TRUE COPY
Dec 07, 2023
s/ Mariah Kauder
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
electronic contents of a cellular telephone, an Apple iPhone with Baltimore Police Department property number 4970008 and two Dell laptops with Baltimore Police Department property numbers 497235 and 497236, which are described in Attachment A

Case No. 23-M-502 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 12-21-23 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 12-7-23. 10:00 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

- The electronic storage of an Apple iPhone with Baltimore Police Department property number 4970008, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

- The electronic storage of a Dell Latitude 7640 laptop, serial number 4VS5BY3 with Baltimore Police Department property number 497235, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

- The electronic storage of a Dell Latitude 5510 laptop, serial number DK0M473 with Baltimore Police Department property number 497236, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

ATTACHMENT B

The following materials, which constitute evidence of the commission of a criminal offense; contraband; the fruits of crime; or property designed, or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2251, Section 2252A, Section 2242, and Section 2243:

1. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

    h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

electronic contents of a cellular telephone, an Apple iPhone with Baltimore Police Department property number 4970008 and two Dell laptops with Baltimore Police Department property numbers 497235 and 497236, which are described in Attachment A

Case No. 23-M-502 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)	Production of Child Pornography
18 U.S.C. § 2252A(a)(1) and 2252A(b)(1)	Transportation of Child Pornography
18 U.S.C. § 2252A(a)(1) and 2252A(b)(2)	Possession of Child Pornography
18 U.S.C. § 2422(a)	Coercion and Enticement of Minors
18 U.S.C. § 2423(a)	Transportation of Minors

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Daniel Gartland, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 12-7-23

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Daniel Gartland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to search the electronic contents of a cellular telephone, an Apple iPhone with Baltimore Police Department property number 4970008 and two Dell laptops with Baltimore Police Department property numbers 497235 and 497236, which are described in Attachment A, for evidence of violations of 18 U.S.C. § 2251, 18 U.S.C. § 2252A, 18 U.S.C. § 2422 and 18 U.S.C. § 2423, which makes it a crime to possess, or knowingly access with intent to view, child pornography, and to knowingly persuade, induce, or transport a minor in interstate commerce with intent to engage in any illegal sexual activity, which is further described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the enticement or kidnapping of children, possession, production, and distribution of child sexual abuse material (commonly known as “CSAM”).

3. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving,

transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have investigated child abduction and child enticement incidents. I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

4. The facts in this affidavit come from my personal observations, training, experience, and/or information obtained from other law enforcement officers and/or witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that on or about November 4, 2023, Said Mukhtar Hamza (XX/XX/1994) used an Apple iPhone, currently secured in evidence with the Baltimore Police Department, property inventory number 4970008, and two Dell laptops, currently secured in evidence with the Baltimore Police Department, property numbers 497235 and 497236, to entice a minor, transport that minor in interstate commerce with intent that the minor engage in illegal sexual activity, produce, possess, and knowingly access child pornography in violation of 18 U.S.C. § 2251(a) – Production of Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1) – Transportation of Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2) – Possession of Child Pornography, 18 U.S.C. § 2422(a) – Coercion and Enticement of Minors, and 18 U.S.C. § 2423(a) – Transportation of Minors. There is probable cause that evidence of those crimes will likely be contained in the electronic contents of an Apple iPhone with Baltimore Police Department property number 4970008 and two Dell

laptops with Baltimore Police Department property number 4975235 and property number 4975236..

DEFINITIONS

6. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B (collectively referred to as "warrant"):

a. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. See United States v. Cross, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); United States v. Riccardi, 258 F.Supp.2d 1212 (D. Kan., 2003) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

f. "Electronic device" includes any electronic, magnetic, optical, electrochemical or other high speed system or device capable of storing and/or processing data in digital form, including but not limited to the following: central processing units; desktop, laptop, and notebook computers; tablets; PDAs; wireless communication devices such as cellular telephones and pagers; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communications devices such as modems, routers, cables and connections; storage media such as hard disk drives, floppy disks, compact disks, flash drives, magnetic tapes and memory chips; security devices; and any data storage facility or communications facility directly related to or operating in conjunction with such device.

g. "Hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to hardware (including physical keys and locks).

h. "Software" is digital information which can be interpreted by an electronic device and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Electronics-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use hardware, software, or other related items.

j. "Passwords and data security components" consist of information or items designed to restrict access to or hide software, documentation, or data. Data security components may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters or symbols) usually operates a sort of digital key to "unlock" data security components. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "Internet Service Providers" (ISPs) are commercial organizations, which provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the internet, web hosting, e-mail, remote

storage, and co-location of computers and other communications equipment. ISPs can offer various means to access the internet, including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, fiber optic cable, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox. The subscriber is then typically required to create a password for the account. By using an internet-capable electronic device, the subscriber and other users can establish digital communication with an ISP and thereby access the internet.

l. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

m. "Internet Protocol address" (IP address) refers to a unique number used by an electronic device to access the internet. IP addresses can be dynamic, meaning the Internet Service Provider (ISP) assigns a different unique number to an electronic device every time it accesses the internet. IP addresses are considered static if an ISP assigns a user's electronic device a particular IP address, which is used each time the device accesses the internet.

n. The terms "records," "documents" and "materials" include all information recorded in any form, visual or audio, and by any means, whether in hand-made form (including writings, drawings, painting); photographic form (including microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including phonograph records, printing, typing); or electrical, electronic or magnetic form (including tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators; and digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but certain attributes may change during the reproduction.

p. "Log Files" are records automatically produced by software to document electronic events that occur on electronic devices. Software can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote electronic devices; access logs list specific information about when an electronic device was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

q. "Cellular telephones" are handheld electronic devices used for wireless voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Emojis" are small digital images or icons used in electronic messages or webpages to communicate an idea, emotion, expression, or feeling. Emojis exist in various genres, including facial expressions, common objects, places, types of weather, and animals.

BACKGROUND ON ELECTRONIC DEVICE USE IN FACILITATING CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION CRIMES

7. Based upon my knowledge, training and experience in online child exploitation and child pornography investigations, as well as the experience and training of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Electronic devices and related technology have revolutionized the way in which child pornography is produced, distributed, viewed, and stored, as well as how it is used in furtherance of online child exploitation.

b. Individuals can convert photographs and videos taken using a traditional camera or video recorder to a format capable of being disseminated quickly and efficiently via the internet using a variety of electronic devices, including scanners, memory card readers, cellular telephones, or directly from digital cameras.

c. Modems and routers allow electronic devices to connect to other devices using telephone, cable, or wireless connections. Electronic contact can be made to literally millions of devices around the world.

d. The capability of electronic devices to store extremely large amounts of high-resolution video and imagery in digital form, which can be password protected or hidden from other device users, makes these devices highly effective at storing child pornography, while also concealing the user's illicit activity.

e. The internet affords individuals many different and relatively secure and anonymous venues for obtaining, viewing, and distributing child pornography; or for communicating with others to do so; or to entice children.

f. Individuals can use online resources to retrieve, store and share child pornography, including services offered by internet portals such as Google, Yahoo!, and Facebook, among others. Online services, which are accessed via electronic device, generally allow a user to set up an account which thereby provides the user with access to email, instant messaging services, online file storage, social media, online message boards, and/or a variety of other interconnected web-based applications. If a user uses any of these functions to obtain, view, store, or distribute child pornography; or for communicating with others to do so; or to entice children, evidence of such activity can often be found on the user's electronic device.

g. As is the case with most digital technology, electronic device communications can be saved or stored on hardware and digital storage media. Storing this information can be intentional, i.e., by saving an e-mail as a file on the electronic device or saving the location of one's favorite websites in, for example, "bookmarked" files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic device user's internet activity generally leaves traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

h. The interaction between software and the electronic device's operating systems often results in material obtained from the internet being stored multiple times, and even in different locations in the device's digital memory, without the user's knowledge. Even if the device user is sophisticated and understands this automatic storage of information, attempts at deleting the material often fail because the

> material may be automatically stored multiple times and in multiple locations within the digital media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's digital media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution, and/or possession of child pornography.

Data that exists on an electronic device is particularly resilient to deletion. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on most electronic devices, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user's operating system, storage capacity, and device habits.

BACKGROUND ON ELECTRONIC EVIDENCE REVIEW/PROCESSING IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATIONS

8. As further described in Attachment B, this warrant seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how electronic devices were used, the purpose of their use, and who used them. Additionally, the warrant seeks information about the possible location of other evidence.

9. Based upon my knowledge, training, and experience, as well as information related to me by law enforcement officers and others involved in the forensic examination of electronic devices, I know that attempting to segregate relevant evidence from non-pertinent information stored on an electronic device, prior to conducting a forensic examination and review of the device, is ineffective in child pornography and online child exploitation investigations. This is true in part because:

a. The items to be searched will not only contain child pornography but will also contain information pertinent to identifying the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography, which may be located throughout the entire areas to be searched.

b. Sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user electronic device) was not a user of the device during the time(s) of the criminal activity. (For instance, based upon my knowledge, training, and experience, as well as information related to me by law enforcement officers and others involved in the forensic examination of electronic devices, I know that when an electronic device has more than one user, files on that device can contain information indicating the dates and times when files were created, as well as the sequence in which they were created. By analyzing this data and comparing it with known historical activity or alibis of the suspected users, law enforcement can establish user identity and exclude others from device usage during times related to the criminal activity. Since the absence of data can only be confirmed via a complete analysis of the device, segregation of the device's data would not be practical or effective.)

c. Although some of the records called for by this affidavit might be found in the form of user-generated documents (such as word processor, picture and movie files), electronic device hard drives can contain other forms of electronic evidence that are not user-generated, which might take a form that becomes meaningful only upon forensic analysis. For instance:

i. Data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

ii. Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes the electronic devices were recently in use.

iii. Web browsers, e-mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords.

iv. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use.

v. Electronic device file systems can record information about the dates files were created and the sequence in which they were created. This information maybe evidence of a crime or indicate the existence and location of evidence in other locations on the hard drive.

10. The types of evidence described above may be direct evidence of a crime; indirect evidence of a crime indicating the location of evidence or a space where evidence was once located; contextual evidence identifying a computer user; and contextual evidence excluding a computer user. These types of evidence may indicate ownership, knowledge, and intent.

11. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging law enforcement officer and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how electronic devices behave and are used. Therefore, contextual information, which is necessary to understand the evidence described in Attachment B, is understood to fall within the scope of the warrant.

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

12. I have consulted in this matter with law enforcement personnel and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. Through this consultation I learned that to properly retrieve and analyze electronically stored computer data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To achieve such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

13. Based on my knowledge, training, and experience, and consultation with forensically trained FBI personnel, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

a. The objects themselves may be instrumentalities used to commit the crime;

b. The objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. The objects may be contraband or fruits of the crime.

14. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device and storage media in particular, computers internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

15. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture,

and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic

and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

16. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") which is read via an integrated biometric device in lieu of a numeric or alphanumeric passcode or password. This feature often referred to as a fingerprint scanner, a fingerprint reader, or for Apple devices, Touch ID.

17. If a user enables the fingerprint scanner on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint scanner, which can be found in different locations on the device depending on the

manufacturer. In my training and experience, users of devices that offer fingerprint scanners often enable it because it is considered a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

18. In some circumstances, a fingerprint cannot be used to unlock a device that has its fingerprint scanner enabled, and a passcode or password must be used instead. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via the fingerprint scanner exists only for a short time. The fingerprint scanner also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) too many unsuccessful attempts to unlock the device via the fingerprint scanner are made.

19. If fingerprint scanner enabled devices are found during a search of the premises, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search of the premises to the device's fingerprint scanner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the device(s) via fingerprint scanner with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

20. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose

fingerprints are among those that will unlock the device via the fingerprint scanner, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the fingerprint scanner of the locked device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via the fingerprint scanner.

21. Based upon my knowledge, training and experience, and consultation with forensically trained personnel, I know that a thorough search for information stored in storage media often requires law enforcement to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting

process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

22. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the law enforcement personnel executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

23. I know that when an individual uses a computer to commit crimes involving child exploitation, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain: data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

SEARCH METHODOLOGY TO BE EMPLOYED

24. As noted within this search warrant, it would be extremely difficult, if not impossible to conduct a thorough on-site review of all potential evidence in this case. Given these constraints, the search methodology to be employed is as follows:

a. All electronic devices and any form of electronic storage that could contain evidence described in this warrant will be seized for an off-site search for evidence described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

b. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative officers.

c. Additional techniques to be employed in analyzing the seized items will include; (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas; (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments; and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

d. Because it is expected that the electronic devices and electronic storage media may constitute, (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case.

e. Because of the large storage capacity as well as the possibility of hidden data within electronic devices and electronic storage media, it is anticipated that there will be no way to ensure that contraband-free evidence could be returned to the user/possessor of the electronic devices and electronic storage media, without first wiping such evidence clean. Wiping the original evidence clean would mean that the original evidence would be destroyed and thus, would be detrimental to the investigation and prosecution of this case.

f. Further, because investigators cannot anticipate all potential defenses to the offenses in this affidavit, and as such, cannot anticipate the significance of the evidence that has been lawfully seized pursuant to this warrant, it is requested that all seized evidence be retained by law enforcement until the conclusion of legal proceedings or until other order of the court.

g. If after careful inspection, investigators determine that such electronic devices and electronic storage media do not contain, (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

CHARACTERISTICS OF INDIVIDUALS INVOLVED

IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION CRIMES

25. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in the possession and distribution of child pornography. Those who possess and distribute child pornography:

a. May receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, electronic storage media, or other visual media. Such individuals often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Often possess and maintain their "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., within their residences, attached or detached garages, associated outbuildings, their vehicles, and/or other secure locations which they maintain dominion and control of, for ready access and to conceal these items from law enforcement, family members, or other individuals who frequent these areas. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, videotapes, and electronic storage media for many years.

d. Often maintain their digital or electronic child pornography collections in a safe, secure, and private environment, such as on an electronic device. These collections are highly valued by the individual, are often maintained for several years, and are kept close by, usually within their residences, attached or detached garages, associated outbuildings, their vehicles, and/or other secure locations which they maintain dominion and control of, for ready access and to conceal these items from law enforcement, family members, or other individuals who frequent these areas.

e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

DETAILS OF THE INVESTIGATION

26. On November 4, 2023, The Kenosha County Sheriff's Department (KCSD) received a complaint from Julie White. She reported that when she awoke at approximately 7:30 a.m., her niece A.E., a 15 year-old minor, was missing from her apartment at 34502 Geneva Road, Burlington, WI. A.E. had stayed with White, while A.E.'s parents were out of town.

27. White fell asleep at approximately 2:00 a.m., after seeing A.E. enter the bathroom of the residence. When White awoke, the bathroom door was still closed, but A.E. was not present. White observed that the bathroom window was closed, but the screen was on the ground outside of the window. White believed A.E. did not have a phone and she could not locate her.

28. A.E. was last seen wearing a black hooded sweatshirt, black leggings, and black and white Nike shoes. A red Christmas blanket was missing from White's residence and was believed to be with A.E.

29. Surveillance video from that night was obtained from businesses in close proximity

to White's apartment building, including Honeydripperz Pub at 34500 Geneva Road, Burlington, WI. The video depicted a silver sedan park in the area of White's apartment at approximately 2:10 a.m. The video depicted a black male appear, consistent with arriving with the vehicle. The black male was wearing dark colored shoes, light colored pants and long dark coat. He walked around in the area of White's apartment building, then returned to the area where the sedan was parked. The sedan then departed.

30. A law enforcement officer from the KCSD interviewed an employee of Honeydripperz Pub on November 7, 2023. The employee departed Honeydripperz Pub while the sedan was still parked in the area. She noted that the sedan had a light up Uber sign.

31. A search warrant was obtained in Kenosha County District Court for devices with Google accounts located in a small geographic area encompassing the location where the sedan parked. Data provided by Google in response to the warrant included Google Subscriber information for Shofu Rahman. A search of law enforcement databases revealed that Rahman resided in Milwaukee, WI. A silver 2013 Hyundai Accent sedan was registered to Rahman.

32. KCSD detectives interviewed Rahman at his home. He stated that he was a driver for both the Uber and Lyft rideshare services. He typically conducted rideshares from the Milwaukee Airport.

33. Rahman allowed KCSD Detectives to review his rideshare applications on his phone. The Lyft application showed that Rahman accepted a rideshare at approximately 12:55 a.m. on November 4, 2023. Rahman drove a passenger from Milwaukee to Burlington, WI, arriving at approximately 2:01 a.m. Rahman was stopped at the location for approximately 15 minutes. Rahman then drove the passenger to back to Milwaukee, arriving at 3:12 a.m.

34. The passenger told Rahman that he was looking for a person in Burlington. When

he could not find the person, Rahman drove him to the Milwaukee Intermodal Station. Upon arriving at the station, the passenger asked Rahman to take him back to Burlington. Rahman stated the passenger's name was "Said."

35. Surveillance video obtained from the Milwaukee Intermodal Tran Station from that same night, located at 433 West St. Paul Avenue, Milwaukee, WI, depicted a black male with a long black coat and dreadlocks enter the building at the approximate time Rahman dropped off his passenger. The individual was observed using his cellular telephone multiple times within the building. At approximately 4:19 a.m., the individual exited the building. At 4:20 a.m., he walked back into the building with a small, white female, wearing a black hooded sweatshirt with the hood up and black pants. The female was carrying a red blanket. Detectives identified the white female as A.E.

36. KCSD detectives conducted a search of A.E.'s home and bedroom with the consent of her mother. Detectives observed drawings with the name "Liam" written on them in A.E.'s bedroom. They also observed a receipt for the food delivery service DoorDash on October 22, 2023. The receipt included customer name "Anna E" and order number "d5a3e2cf-ce".

37. On November 9, 2023, DoorDash, Inc. responded to an exigent request for information regarding DoorDash order number d5a3e2cf-ce. The information provided identified A.E. as the customer. The phone number associated with the order was 816-389-7550. The email address associated with the order was kaidawhite03@gmail.com. The order was paid for via a Visa credit card with the last four digits of 9160.

38. KCSD detectives also located a daily planner in one of A.E.'s backpacks. The word "Liam" was written in the planner on November 3, 2023. A heart was drawn around the name. The phrase "out of state" was also written in the planner near November 3, 2023.

39. KCSD detectives interviewed A.E.'s minor friend S.F. in the presence of S.F.'s parents. S.F. knew A.E. to be communicating with older males online. S.F. knew one of the older males A.E. talked to was named "David." S.F. knew A.E.'s Snapchat account name to be, "Lunny_toons420".

40. KCSD detectives interviewed A.E.'s minor friend B.L. in the presence of B.L.'s mother. B.L knew A.E. communicated with older men via Instagram and Snapchat. A.E. told B.L. that one of the people A.E. was speaking to could help her get away from her family. Approximately one week prior to A.E.'s disappearance, A.E. told B.L. that she planned to run away to Maryland.

41. KCSD detectives interviewed A.E.'s minor friend A.V. in the presence of A.V.'s parents. A.E. told A.V that she met a male online who had a wife and son her age and that they offered to take A.E. into their home. The person A.E. met online lived in Maryland and the son was African American. A.E. talked about the name "Liam." A.V. was unsure if it was the name of the person A.E. was talking to or the son. A.E. told A.V. the husband was going to fly to Milwaukee, Anna was going to meet him there, and they would ride back to Maryland together. A.E. told A.V. the man had given her his credit card to order food from DoorDash.

42. A.V. told detectives that A.E. had a phone that she kept hidden from her parents. A.V. received a message via Snapchat from A.E. on November 4, 2023. The message stated that A.E. was in Milwaukee and that she loved her. A.V. believed A.E. planned to destroy her phone and discontinue contact with her friends for three months.

43. A search warrant was obtained in Kenosha County District Court for A.E.'s Snapchat account, "Lunny_tunes420". Snapchat provided information in response to the search warrant on November 9, 2023. Detectives observed the date of birth for the account owner to be

the same as A.E.'s date of birth. The information also indicated the account was last active on November 4, 2023.

44. Detectives observed that A.E. added Snapchat account "liaminca" as a friend on August 28, 2023. The same user was removed as a friend on November 6, 2023. Portions of communications between A.E. and Snapchat user "liaminca" were provided by Snapchat in response to the search warrant. Detectives observed images of lingerie, underwear and bras that "liaminca" sent to A.E. Based upon my training and experience, I know individuals that send images of lingerie and undergarments to minors, will often entice those minors to progressively produce images of themselves in lingerie, nude or sexual images of themselves. Those individuals then retain those images on phones or in other electronic storage devices.

45. They also observed a satellite image sent from A.E. to "liaminca". The image included A.E.'s residence at 34517 Geneva Road, Burlington, WI, which was marked, "where I live." A red line from A.E.'s residence to a black dot were overlayed onto the image. The red line included the text, "way I'll take" and the black dot included the text, "where we meet." The words, "where you park" overlayed the parking lot at Best Bargains, 6515 352nd Avenue, Burlington, WI, 53105.

46. Detectives observed the avatar of the "liaminca" Snapchat account was a black male with dreadlocks. An open-source search of multiple social media platforms was conducted for account names similar to "liaminca". The username "liaminca" was located on the Kik messaging platform. The profile image associated with the account was a black male with dreadlocks. The image was consistent with the black male observed on surveillance video in the area of White's apartment building.

47. Detectives submitted the profile photo of Kik user "liaminca" to the Mid-States

Organized Crime Information Center (MOCIC). MOCIC used facial recognition software to identify a photo associated with the Facebook account "Blaise Dk". Detectives reviewed posts associated with the account. The Facebook page "Mina Abdusssabur" posted a photo of the same black male with the caption, "Because I have a Black Son".

48. A search of law enforcement databases produced a result for a Mina Abdussabur with ties to Baltimore, Maryland. Abdussabur also had potential relatives by the names of Said A Hamza, Said Hussain Hamza, and Said Mukhtaar Hamza.

49. A search of law enforcement databases was conducted for information related to Said Mukhtaar Hamza (XX/XX/1994). He was associated telephone number 816-389-7550, the same number associated with the DoorDash order receipt recovered from A.E.'s bedroom. Hamza was also associated with several addresses in Baltimore, Maryland.

50. Information was requested from the Greyhound Bus Lines for any tickets purchased by Said Mukhtaar Hamza on November 4, 2023. Greyhound Bus Lines provided ticket information for two passengers, "Said Hamza" and "Anna Estesa". The tickets departed the Milwaukee Bus Station, 433 West St. Paul Avenue, Milwaukee, WI, at 6:40 a.m. on November 4, 2023 and arrived in Baltimore, Maryland on November 5, 2023 at approximately 8:25 p.m.

51. KCSD Detectives issued a temporary felony warrant for Said Mukhtaar Hamza for violations of Wisconsin state statutes 940.31(1)(c), Felony Kidnapping, and 948.30(1)(a), Felony Abduction of a Child.

52. An exigent request for information was submitted to AT&T Wireless for Timing Advanced Data records for telephone number 816-389-7550 for November 4, 2023. An analysis of the records revealed the telephone was located at the Milwaukee Mitchell International Airport at approximately 1:00 a.m. on November 4, 2023. The phone then traveled to an area near Julie

White's residence in Burlington, WI, arriving at approximately 2:20 a.m. The device then returned to an area encompassing the Milwaukee Intermodal Station, arriving at approximately 3:10 a.m. The device departed the area at approximately 7:17 a.m., moving in a direction consistent with travel along U.S. Interstate 43 and U.S. Interstate 94.

53. KCSD Detectives contacted the Baltimore Police Department for assistance in recovering A.E. and arresting Said Mukhtaar Hamza.

54. KCSD Detectives obtained a search warrant in Kenosha County District Court for the Snapchat account "liaminca". Snapchat provided information in response to the search warrant on November 9, 2023. Detectives observed the date of birth for the account owner to have the same month and day as Hamza with a different birth year of 2005. The phone number associated with the account was 816-319-7550. Detectives observed multiple selfie-style images associated with the account. Based upon my trained and experience, I believe Hamza used an incorrect birth year when establishing his Snapchat account to imply a younger age when communicating with minors via Snapchat.

55. Detectives observed a photo from November 5, 2023 which depicted A.E. and Said Mukhtaar Hamza on a bus. Communications between "liaminca" and A.E. were included in the records provided by Snapchat. One such communication appeared to discuss age, but only included A.E.'s messages. A.E. stated, "15," followed by a question regarding liaminca's age. A.E. then stated, "You don't look 25, I thought you were 16."

56. The Snapchat records included communications between "liaminca" and other Snapchat users. During one such communication with a user believed to be from Austria, liaminca stated, I've never been but you look like a good reason to visit…..You laugh but I'd kidnap you frfr."

57. On November 10, 2023, Said Mukhtaar Hamza was taken into custody by the Baltimore Police Department at 3912 10th Street, Baltimore Maryland. A.E. was located within the residence, unclothed. Detectives observed that A.E. appeared to have hematomas, more commonly referred to as "hickeys," on her neck.

58. On November 10, 2023, a Baltimore Police Detective conducted a custodial interview of Said Mukhtaar Hamza. After being advised of his Miranda rights and waiving those rights, Hamza agreed to speak with the Detective. Hamza stated that he met A.E. through an online dating application several months prior. Hamza and A.E. made a plan for her to come to Baltimore. Hamza traveled to Wisconsin, transported A.E. away from her home using a ride share application, then traveled with her via bus to Baltimore. Hamza stated that, once in Baltimore, he engaged in sexual intercourse with A.E. an unknown number of times.

59. On November 10, 2023, the Baltimore Police Department executed a search warrant at 3912 10th Street. During the search, the following items were located in a bedroom believed to belong to Hamza:

- Two Dell laptops,
- Bedding, including one comforter and one sheet,
- Assorted credit cards, and
- One black in color iPhone.

Among the assorted credit cards was a card in the name of Said Hamza. The last four digits of the card were 9160, which matched the last four digits of the card on the DoorDash receipt recovered in A.E.'s bedroom. Hamza's government identification was also recovered from the room. The iPhone was submitted to the Baltimore Evidence Control Unit under property number 4970008. The two Dell laptops were submitted to the Baltimore Evidence Control Unit under property

number number 4975235 and property number 4975236.

60. On November 15, 2023, a Baltimore Police Detective obtained a warrant to search the iPhone for evidence of violations of Maryland Criminal Law Code CR 3-324 Sexual Solicitation of Minor, CR-503(a) Kidnapping of a child under 16, and CR3-307 Sex Offense Third Degree. The Baltimore Police Department attempted to execute the warrant by conducting a forensic download of the device. The attempt was not successful, and the device remains in the custody of the Baltimore Police Department. Prior to conducting the forensic download, a manual preview of the device was conducted. Various images of Hamza and A.E. in a bed were observed on the phone. The Federal Bureau of Investigation agreed to conduct a forensic download of the device in support of a federal investigation into the incident. The warrant obtained by the Baltimore Police Department does not contain the appropriate language that would allow federal agents to execute the warrant.

BIOMETRIC ACCESS TO DEVICES

61. This warrant permits law enforcement to compel residents of the PREMISES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints

that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, I believe one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such

features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Brandon Gilmore or other PREMISES's residents to the fingerprint scanner of the devices; (2) hold the devices found in front of the face of Brandon Gilmore or other PREMISES's residents and activate the facial recognition feature; and/or (3) hold the devices found in front of the face of Brandon Gilmore or other PREMISES's residents and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Brandon Gilmore or other PREMISES's residents state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel Brandon Gilmore or other PREMISES's residents to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

62. Based on the foregoing, there is probable cause to believe that Said Mukhtaar Hamza utilized an Apple iPhone with Baltimore Police Department property number 4970008, and two Dell laptops with Baltimore Police Department property numbers 497235 and 497236, in violation of 18 U.S.C. § 2252A, 18 U.S.C. § 2422, and 18 U.S.C. § 2423, which, among other things, makes it a federal crime for any person to possess, or knowingly access with intent to view, child pornography, and to knowingly persuade, induce, or transport a minor in interstate commerce with intent to engage in any illegal sexual activity, and that the property, evidence, fruits and

instrumentalities of these offenses, more fully described in Attachment B, are located in the electronic contents of an Apple iPhone with Baltimore Police Department property number 4970008, and two Dell laptops with Baltimore Police Department property numbers 497235 and 497236, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

ATTACHMENT A

- The electronic storage of an Apple iPhone with Baltimore Police Department property number 4970008, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

- The electronic storage of a Dell Latitude 7640 laptop, serial number 4VS5BY3 with Baltimore Police Department property number 497235, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

- The electronic storage of a Dell Latitude 5510 laptop, serial number DK0M473 with Baltimore Police Department property number 497236, seized from 3912 10th Street, Baltimore, Maryland, which is currently in the custody of the Baltimore Police Department.

ATTACHMENT B

The following materials, which constitute evidence of the commission of a criminal offense; contraband; the fruits of crime; or property designed, or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2251, Section 2252A, Section 2242, and Section 2243:

1. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

    e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

    f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

    g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

    h. evidence of the times the electronic storage device was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.